Daily Open Source Infrastructure Report
29 July 2015

Top Stories

- Fiat Chrysler Automobiles issued a recall for about 1 million Ram pickup trucks due to an issue with the steering wheel wiring harness and another separate recall for 843,536 Ram vehicles due to an issue with the truck's Occupant Restraint Control module. – *Car Connection* (See item **4**)

- The owner of Stanfill Wealth Management in Knoxville was charged July 27 after allegedly defrauding over 21 investors out of almost $7 million. – *WBIR 10 Knoxville* (See item **5**)

- Oregon State Police reported July 27 a statewide investigation had begun after 10 government offices received mail containing a suspicious substance that hospitalized a sheriff and prompted the evacuation of several locations. – *KATU 2 Portland* (See item **17**)

- A July 26 wildfire destroyed a mobile home and prompted the evacuation of 400 Clearlake residents from the Cache Creek Apartment complex. – *Santa Rosa Press Democrat* (See item **31**)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH
- Food and Agriculture
- Water and Wastewater Systems
- Healthcare and Public Health

SERVICE INDUSTRIES
- Financial Services
- Transportation Systems
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE
- Government Facilities
- Emergency Services

Energy Sector

1. *July 27, San Francisco Chronicle* – (California) **S.F. Muni to pay $525,000 for underground fuel tank violations.** State regulators announced July 27 a $525,000 settlement with the Municipal Transportation Agency (MTA) after a 2012 investigation revealed the agency violated leak-protection requirements for underground fuel storage tanks at 4 Muni yards in San Francisco. The MTA will be required by the Water Resources Control Board to develop and follow a leak prevention program for five years or face further penalties.
Source: http://www.sfgate.com/bayarea/article/S-F-Muni-to-pay-525K-over-latest-underground-6408739.php

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *July 27, Minneapolis Star Tribune* – (Minnesota) **Feds allege Xcel contractors falsified weld tests at Monticello nuclear plant.** The U.S. Nuclear Regulatory Commission charged two former contract employees of Xcel Energy Inc., with willfully violating procedures and falsifying reports about safety-related tests of casks filled with high-level nuclear waste stored at the Monticello, Minnesota nuclear power plant July 27.
Source: http://www.startribune.com/feds-allege-xcel-contractors-falsified-weld-tests-at-monticello-nuclear-plant/318734611/

3. *July 27, Chattanooga Times Free Press* – (Tennessee) **Sequoyah Nuclear Power Plant unit 1 trips again.** Officials reported that the Unit 1 reactor at the Sequoyah Nuclear Power Plant was shut down July 27 due to a fluctuation in the voltage output from the plants generator. The shutdown did not endanger employees or the public, and crews are working to restore the reactor.
Source: http://www.timesfreepress.com/news/business/aroundregion/story/2015/jul/27/sequoyah-unit-2-trips-again/316768/

Critical Manufacturing Sector

4. *July 27, Car Connection* – (National) **2012-2015 Ram pickups recalled to fix seatbelts, airbags; 1.9 million vehicles affected.** Fiat Chrysler Automobiles issued a recall for about 1 million model year 2012 – 2014 Ram pickup trucks due to an issue with the steering wheel wiring harness that could cause potential inadvertent driver side air bag deployment, and a separate recall for 843,536 model year 2013 – 2015 Ram vehicles due to an issue with the truck's Occupant Restraint Control module that could cause side curtain and seat airbags to deploy and seatbelt pretensioners to activate unexpectedly.
Source: http://www.thecarconnection.com/news/1099289_2012-2015-ram-pickups-recalled-to-fix-seatbelts-airbags-1-9-million-vehicles-affected

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *July 28, WBIR 10 Knoxville* – (Tennessee) **Fraud victims speak out after financial adviser indicted, arrested.** Authorities unsealed indictments against the owner of Stanfill Wealth Management July 27 in Knoxville, alleging that she defrauded over 21 investors out of almost $7 million by promising to invest funds in Charles Schawb and Co., and instead diverted the money for her personal use.
Source: http://www.wbir.com/story/news/2015/07/27/former-financial-adviser-jacqueline-stanfill-indicted-on-federal-fraud-counts/30741685/

For another story, see item **16**

Transportation Systems Sector

6. *July 28, WHIO 7 Dayton* – (Ohio) **I-70 east reopens after semi hits unattended car.** All lanes of Interstate 70 in Englewood have reopened July 28 after being shut down for over 2 hours while crews cleared the scene of an accident after a semi-truck struck an unattended disabled vehicle and injured 1 person.
Source: http://www.whio.com/news/news/traffic/jackknifed-semi-crash-shuts-down-i-70/nm7hM/

7. *July 28, WITI 6 Milwaukee* – (Wisconsin) **United Express plane makes emergency landing at Mitchell International.** A United Express flight made an emergency landing and returned to Mitchell International Airport in Milwaukee shortly after departure due to a mechanical problem.
Source: http://fox6now.com/2015/07/28/united-express-plane-makes-emergency-landing-at-mitchell-international-airport/

8. *July 28, WVIT 30 3 New Britain* – (Connecticut) **Dad and son killed in fiery truck crash on I-95 in Stonington.** The northbound lanes of Interstate 95 in Stonington reopened July 28 after a semi-truck crashed and caught on fire July 27, killing the truck's two passengers.
Source: http://www.nbcconnecticut.com/news/local/Tractor-Trailer-Fire-Closes-I-95-North-in-Groton-318727331.html

9. *July 27, Consumerist* – (Texas) **Man arrested after making it through security, boarding plane without ticket.** The DHS Transportation Security Administration (TSA) is investigating a July 26 incident at the Dallas Fort-Worth International Airport in which a man was arrested after he made his way through a TSA checkpoint and to an airport gate without a ticket. An airline agent alerted authorities of the unticketed passenger and a bomb squad was called to check the man's vehicle.
Source: http://consumerist.com/2015/07/27/man-arrested-after-making-it-through-

security-boarding-plane-without-ticket/

10. *July 26, WNEW 99.1 FM Washington, D.C.* – (Washington, D.C.) **Fatal crash shuts down SE-SW Freeway.** The Southeast-Southwest Freeway in the District of Columbia was shut down for several hours July 26 due to a single-vehicle crash that killed 1 person and injured another.
Source: http://washington.cbslocal.com/2015/07/26/fatal-crash-shuts-down-se-sw-freeway/

Food and Agriculture Sector

11. *July 27, Associated Press* – (National) **FDA bans some Mexican cilantro after human feces found in fields.** The U.S. Food and Drug Administration reported July 27 that fresh cilantro from Puebla, Mexico was partially banned after a federal government investigation found human feces and toilet paper in Mexico's growing fields. The product was linked to a 2013 –2014 outbreak of stomach illness in the United States.
Source: http://www.huffingtonpost.com/entry/fda-ban-mexico-cilantro-contaminated_55b6d57ee4b0a13f9d1a0297

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

12. *July 28, Associated Press* – (Illinois) **Mumps outbreak centered at U of Illinois.** The Illinois Department of Public Health announced July 28 that the State has 73 cases of mumps, most of which are centered at the University of Illinois campus in Champaign County making this case the largest mumps outbreak in over a decade.
Source: http://fox2now.com/2015/07/28/mumps-outbreak-centered-at-u-of-illinois/

13. *July 28, Atlanta Business Chronicle* – (Georgia) **Patient information released in Georgia agency data breach.** The Georgia Department of Human Services Division of Aging Services notified approximately 3,000 people served by the agency's Community Care Services Program of a data breach involving health diagnoses through an email to a contracted provider July 28.
Source: http://www.bizjournals.com/atlanta/morning_call/2015/07/patient-information-released-in-state-agency-data.html

14. *July 27, Securityweek* – (New York) **Healthfirst: 5,300 members exposed in fraud incident.** Healthfirst, which provides care to over one million members in New York, announced July 24 that nearly 5,300 of its current members had personal information compromised after a hacker gained access to the company's online portal April 11, 2012 – March 26, 2014. A suspect has been identified and charged with fraud, and those affected will be provided free identity theft, credit monitoring, and credit restoration services for one year.
Source: http://www.securityweek.com/healthfirst-5300-members-exposed-fraud-

incident

15. *July 27, Columbus Dispatch* – (Ohio) **Patient data included on missing thumb drive, OhioHealth says.** OhioHealth Riverside Methodist Hospital announced July 24 the potential breach of sensitive data for 1,006 valve-replacement candidates and research subjects after an unencrypted flash drive was found missing May 29. Hospital officials do not believe the flash drive was stolen or used inappropriately, and OhioHealth is transitioning to encrypted flash drives in hospitals throughout the State.
Source: http://www.dispatch.com/content/stories/local/2015/07/27/OhioHealth-thumb-drive-missing.html

Government Facilities Sector

16. *July 27, HousingWire.com* – (New York) **NY State senator convicted in foreclosure embezzlement scheme.** A New York State senator vacated his senate seat July 24 after being convicted of obstruction of justice and making false statements to Federal agents, stemming from charges that he embezzled funds held in escrow from the sale of real estate properties.
Source: http://www.housingwire.com/articles/34588-ny-state-senator-convicted-in-foreclosure-embezzlement-scheme

17. *July 27, KATU 2 Portland* – (Oregon) **Statewide investigation underway after government offices receive suspicious mail.** Oregon State Police announced July 27 a statewide investigation after at least ten government offices received mail containing a suspicious substance, sparking the evacuation of several locations, and hospitalizing a sheriff who opened one of the letters at the Grant County Correctional Facility. A U.S. Postal official believe the letters are related but do not believe the general public is at risk.
Source: http://www.katu.com/news/local/Statewide-investigation-underway-after-government-offices-receive-suspicious-mail-318723211.html

18. *July 27, Los Angeles Times* – (California) **Fire closes parts of Pasadena Courthouse; some cases transferred.** A July 27 fire caused by oil-soaked rags closed parts of the Pasadena Courthouse through July 28, redirecting many cases to Boyle Heights and downtown Los Angeles. The clerk's office remained open, and traffic cases took place as scheduled.
Source: http://www.latimes.com/local/lanow/la-me-ln-courthouse-fire-pasadena-20150727-story.html

For another story, see item **12**

Emergency Services Sector

For another story, see item **31**

Information Technology Sector

19. *July 28, Softpedia* – (International) **One in 600 Web sites lists its .git folder, exposing sensitive data.** A Web developer discovered that out of 1.5 million Web sites scanned, 2,402 had an inadvertently exposed .git folder, possibly exposing sensitive information.
Source: http://news.softpedia.com/news/one-in-600-websites-lists-its-git-folder-exposing-sensitive-data-487934.shtml

20. *July 28, Securityweek* – (International) **Cybercriminals use Angler exploit kit to target PoS systems.** Trend Micro researchers reported that cybercriminals have been utilizing the Angler exploit kit (EK) to deliver a reconnaissance trojan that detects mitigation tools before downloading one of three point-of-sale (PoS) malware payloads.
Source: http://www.securityweek.com/cybercriminals-use-angler-exploit-kit-target-pos-systems

21. *July 28, IDG News Service* – (International) **Over 10 million Web surfers possibly exposed to malvertising.** Cyphort released tracking data from malicious advertisement campaigns revealing that since July 18, over 10 million people may have visited Web sites containing malicious ads which redirect visitors to directories hosting the Angler exploit kit (EK).
Source: http://www.computerworld.com/article/2953256/security/over-10-million-web-surfers-possibly-exposed-to-malvertising.html#tk.rss_security

22. *July 28, Softpedia* – (International) **Darkode forum returns with enhanced security measures.** MalwareTech researchers reported that the Darkode hacker forum was back online with enhanced security and authentication processes to prevent future infiltrations, after July raids by the FBI and international partners led to the shutdown of the Web site and the detainment of multiple individuals associated with it.
Source: http://news.softpedia.com/news/darkode-forum-returns-with-enhanced-security-measures-487966.shtml

23. *July 28, SC Magazine* – (International) **Apple App Store and iTunes buyers hit by zero-day.** Security researchers from Vulnerability Lab published a zero-day filter bypass flaw in Apple's online invoicing system used in its App Store and iTunes that could allow an attacker to hijack a user's purchasing session to buy and download any app or content they want, before charging it to the original user.
Source: http://www.scmagazineuk.com/apple-app-store-and-itunes-buyers-hit-by-zero-day/article/428864/

24. *July 28, Network World* – (International) **Software vulnerabilities hit a record high in 2014, report says.** Secunia released analysis from its Vulnerability Review 2015 revealing that the number of recorded software vulnerabilities hit a record high of 15,435 in 2014, an increase of 18 percent from the previous year, and that many organizations are too slow to release security fixes, among other findings.
Source: http://www.networkworld.com/article/2953304/security/software-vulnerabilities-on-the-rise-record-high-report.html#tk.rss_all

25. *July 27, Dark Reading* – (International) **Phishing attacks drive spike in DNS threat.** Infoblox and Internet Identity published data revealing that the Domain Name System (DNS) Threat Index jumped nearly 60 percent in the second quarter of 2015, reportedly due to a corresponding 74 percent increase in phishing and phishing domains over the same period.
Source: http://www.darkreading.com/attacks-breaches/phishing-attacks-drive-spike-in-dns-threat/d/d-id/1321480

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

For another story, see item **23**

Commercial Facilities Sector

26. *July 28, WFSB 3 Hartford* – (Connecticut) **Three firefighters hurt in stubborn Hartford apartment fire.** A 3-alarm fire prompted the evacuation of about a dozen families from a Hartford apartment building after starting on the first floor and spreading to surrounding units. About 60 firefighters remained on site for over 2 hours containing the incident, leaving 3 firemen injured.
Source: http://www.wfsb.com/story/29646067/crews-battling-heavy-fire-on-park-street

27. *July 28, WLS 7 Chicago* – (Illinois) **Bridgeport extra-alarm fire extinguished; witnesses heard explosion.** Officials reported July 28 that DiFoggio Plumbing & Sewer Contractors Inc., sustained extensive damage after an extra-alarm fire destroyed a portion of the building and roof rented by J&J Services. No injuries were reported.
Source: http://abc7chicago.com/news/bridgeport-fire-extinguished;-witnesses-heard-explosion/888155/

28. *July 27, WJAR 10 Providence* – (Rhode Island) **Warwick movie theater evacuated following fire alarm.** A fire alarm at the Showcase Cinemas in Warwick, Rhode Island forced the evacuated of the entire building July 27 and deployed three fire trucks to respond to the scene. It is unknown what caused the alarm to sound.
Source: http://www.turnto10.com/story/29644601/warwick-movie-theater-evacuated-following-fire-alarm

29. *July 27, WPVI 6 Philadelphia* – (New Jersey) **Apartment fire forces evacuation of 350 people in Pennsauken Twp.** Over 350 residents were evacuated July 27 after a fire at the Cooper River Plaza apartments in Pennsauken, New Jersey spread throughout the 14-story building. Firefighters contained the incident and an

investigation is ongoing to determine the cause.
Source: http://6abc.com/news/apartment-fire-forces-evacuation-of-350-people-in-nj/886000/

30. *July 27, KTVX 4 Salt Lake City* – (Utah) **Fire near Jordanelle causes evacuation of homes.** A 2-acre brush fire in Wasatch County, Utah prompted the evacuation of residents at the Fox Bay Condominiums after gusty winds increased the flames towards residential areas July 27. Fire crews remained on site for three hours containing the incident.
Source: http://www.ksl.com/?nid=148&sid=35683877

31. *July 27, Santa Rosa Press Democrat* – (California) **Clearlake fire forces evacuation of 400.** A wildfire destroyed a mobile home and prompted the evacuation of surrounding homes in Clearlake and 400 residents at the Cache Creek Apartment complex July 26. Over 123 firefighters, 14 engine companies, 2 tankers, and 6 helicopters helped contain the incident.
Source: http://www.pressdemocrat.com/news/4261289-181/clearlake-fire-forces-evacuation-of

Dams Sector

Nothing to report

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer